Maryland Patch Management Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

Patch Management is a proactive practice designed to prevent exploitation of known vulnerabilities within an organization's IT infrastructure. An effective patch management process helps mitigate the costs of time and effort expended defending against vulnerabilities known to the information security field at large. Timely patching of known security issues is recognized as a best practice critical to maintaining the confidentiality, availability, and integrity of information systems. The time immediately after the release of a patch is a particularly vulnerable moment for organizations because the window of time between obtaining, testing, and deploying a patch to the vulnerable IT Systems is sufficient for malicious entities to attempt various exploitation strategies. To increase efficiency, the Maryland Department of Information Technology (DoIT) will utilize the baseline controls and standards established by NIST SP 800-53R4, 800-40R2, and 800-40R3 to develop its Patch Management Policy.

2.0 Document and Review History

This policy supersedes the DoIT Patch Management Policy (June 2014) and any other related policies concerning patch management, including sections of the Maryland Information Security Policy (version 3.1, Feb 2013) and other policies declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all **Information Technology Assets** utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. Information Technology Assets include any systems and applications with software or firmware updates provided by a vendor or developer in response to functional or code improvements, flaw or interoperability issues, or version/feature updates.

4.0 Policy

This policy describes an overall strategy to implement timely patch management processes within the State Executive infrastructure.

4.1 Patch Management Group

The Maryland Department of Information Technology (DoIT) will establish the Enterprise Patch Management Group that will be responsible for creating, maintaining, and reviewing a documented patch management process that identifies, reports, and corrects known vulnerabilities of assets authorized to connect to/operate on the DoIT Enterprise network. This group will maintain the confidentiality, integrity, and availability of IT Assets of State agencies under direct DoIT management by ensuring systems are updated with newly released vendor patches within a reasonable period of time, identified in section 4.4.

Agencies under the policy authority, but not under direct management, of DoIT must comply with the requirements of this policy by designating an internal Patch Management Group which will coordinate with the Enterprise Patch Management Group to establish an effective remediation process as required by this policy.

4.2 Requirements for Security Patches

Patch Management Groups (i.e., the Enterprise Patch Management Group and all internal Patch Management Groups) will establish a documented patch management process to address the deployment of **security related patches**. This process, described more fully in NIST SP800-40R2, must entail:

1. A methodology for discovering and tracking IT Assets, which include ensuring all assets are inventoried properly and meet the minimum standards described in the configuration management approved baseline for hardware, software, and applications;
2. Active monitoring of security sources for vulnerability announcements, patch and non-patch remediation, and emerging threats that correspond to the software within the DoIT system configuration (See Appendix A);
3. Establishing a priority for remediation, such as critical security patches requiring remediation within x hours/days/weeks upon patch release (detailed in section 4.4);
4. Establishing a database or inventory of updates applicable to the organization;
5. Performing testing of patches within a lab environment or within a core group of test machines to ensure patch functionality within the infrastructure (ensuring updates do not cause interoperability issues);
6. Scheduling full Enterprise remediation either through automated tools or coordinate with subordinate agencies to comply within a reasonable timeline;
7. Addressing and remediating disconnected or failed machine updates;
8. Conducting periodic vulnerability scanning to identify non-compliant assets for remediation.

4.3 Patch Management Prioritization

4.3.1 Asset Classification

In order to effectively deliver patches to systems, assets need to be identified according to the *Asset Management Policy* and classified according to *Security Assessment Policy*. Utilizing an automated management tool, assets must be discovered and identified as an authorized device before gaining access to the network. Assets with non-routine connections (such as deployed laptops) are required to connect to the network at least once per month to receive updates. All assets must be remediated to the current approved patch cycle before gaining access to the network. Assets categorized with a higher security priority must be patched within a designated timeline according to section 4.4.

Any discovered assets not identified in the Asset Inventory must be tracked and investigated. Any unauthorized device on the network constitutes a security event as defined in the *Cybersecurity Incident Response Policy*, and subject to the enforcement section of that policy.

4.3.2 Patch Category

Additionally, patch management must be prioritized based on the severity of the vulnerabilities the patch addresses. The Patch Management Group shall use the **Common Vulnerability Scoring System (CVSS)** or a directly compatible alternative. Severity scores are categorized in the table below:

Vulnerability Severity	CVSS Severity Score
High	7 – 10
Medium	4 – 6.9
Low	0 – 3.9

4.4 Patch Management Timeline

The applicable Patch Management Group will assign patches a priority level based on the risk classification of each asset and the patch category. To the extent possible, the patching process must follow the timeline in the table below:

Priority Level	Patch Initiated	Patch Completed
1	Within 48 hours of patch release	Within 1 week of patch release
2	Within 1 week of patch release	Within 1 month of patch release
3	Within 1 month of patch release	Within 2 months of patch release

Timeliness of patch management prioritization may be impacted by several factors, including:

- Consideration of asset classification and data affected by the vulnerability
- Stricter requirements set by regulatory standards (such as HIPAA and PCI DSS)
- Discretion of CISO or delegated authority regarding the potential risk to the environment

4.5 Requirements for Non-Security Patches

Timely implementation of **non-security related patches** should be conducted to mitigate against degradation of functionality and/or interoperability. Examples of non-security patches include software updates to increase functionality. The applicable Patch Management Group will establish a documented patch management process to address the deployment of non-security patches. This process will meet the following requirements:

- Deployment of security patches is to be prioritized over non-security patches, where possible;
- Test for the stability and functionality of patches before deployment;
- Incorporate non-security patch management into the organizational configuration management process;
- Require the use of the same patch management solution as for security related patches, where possible.

4.6 Change Management Requirements

4.6.1 Requirements for Patch Deployment

All patch implementations will adhere to configuration management processes regarding submission of documentation related to making system changes. Standard patch deployments will be classified as low-risk configuration changes and must be submitted to the Configuration Manager for review once patches relevant to the organization's IT Assets have been identified. This documentation will be standardized to encourage ease of submission while complying with configuration management baseline requirements defined in the *Configuration Management Policy*.

4.6.2 Approved Baseline Gold Image Requirements

Approved Baseline Gold Images for servers and workstations will be updated at least biannually to maintain the timeliness of the approved baseline configuration defined in the *Configuration Management Policy*. Updating the Gold Image ensures newly deployed assets are built to a level of security documented in the approved baseline and minimizes the time spent updating the asset to the current patch cycle.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Other related policies include:

- Asset Management Policy
- Configuration Management Policy
- Cybersecurity Incident Response Policy
- Security Assessment Policy

7.0 Definitions

Term	Definition
Common Vulnerability Scoring System (CVSS)	An open framework for communicating the characteristics and impacts of IT vulnerabilities which ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.
Information Technology Assets	The collection of networked devices and infrastructure systems critical to the business functionality of the State of Maryland or protecting the resources used or operated by the State. These assets are typically inventoried and audited/accounted for periodically and include servers, virtual servers, desktop workstations, laptops, printers/scanners, VoIP systems, telecomm assets, security (such as CCTV or entry control systems), and offline or SCADA-type systems.
Non-Security Related Patch	A widely released fix for a specific problem, addresses a noncritical, non-security-related bug or a new product functionality that is first distributed outside the context of a product release.
Patch Management	The process for identifying, acquiring, installing, and verifying patches for products and systems.
Security Related Patch	A widely released fix for a product-specific, security-related vulnerability, rated by severity.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for patch management of Enterprise onboarded agencies. DoIT will manage patches according to established requirements authorized in the DoIT Cybersecurity Program Policy and described in this policy's Section 4.0. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies. Any agencies under the policy authority of DoIT with requirements that deviate from the DoIT Cybersecurity Program policies are required to submit a Policy Exemption Form to DoIT for consideration and potential approval.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority,

may extend a non-compliant agency's window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant.

Administrators and IT staff are required to ensure that they monitor, remediate, and address issues related to patch management. Systems found to be out of compliance will be forced to update. Any attempt to circumvent this patch policy by any personnel or agency will be treated as a security violation and subject to investigation. The results of the investigation may entail written notice, suspension, termination, and possibly criminal and/or civil penalties.

Appendix A: Security Sources for Patch Information

Automated Patch Management Tools:

Automated Patch Management Tools perform scheduled requests to vendors to receive notification of pending updates, which in turn notify the patch administrators. Upon notification, patch administrators can begin the patch management process.

Vendor Websites:

Vendor Websites can be searched and reviewed by patch administrators to determine application, software, or firmware updates. In the case of a management tool incapable of discovering or remediating certain assets, such as printer/scanners, administrators will need to schedule a periodic review of vendor websites for non-managed assets, or enroll in a vendor provided notification method, such as registering for vendor email notifications.

Vulnerability Scanners:

Vulnerability Scanners perform assessments of discovered assets based on the current list of threat definitions. Personnel assigned to perform vulnerability scans will ensure the tool has the latest definitions before scanning, and upon completion of scans will report compliance findings to the applicable Patch Management Group for remediation.

Penetration Tests:

Penetration Testing is a method of actively conducting unauthorized attempts to access the systems using a variety of attack strategies. The constraints of these tests as well as who will be authorized to perform them will be determined by the cybersecurity management and scheduled as needed. The results of these tests will be reported to management and remediation of these findings will be determined, which may include the patching of vulnerable systems.

Threat Intelligence:

By monitoring threat intelligence information feeds, cybersecurity personnel can begin devising methods of detecting exploitation of vulnerabilities for which vendors may not have developed a patch. Patch administrators can begin a planning phase for remediating vulnerable assets upon release of the required patch, while network defense personnel can institute a monitoring policy for assets the threat may exploit.